

System Design

1. System Architecture

2. Data Flow Diagram

3. Component Diagram

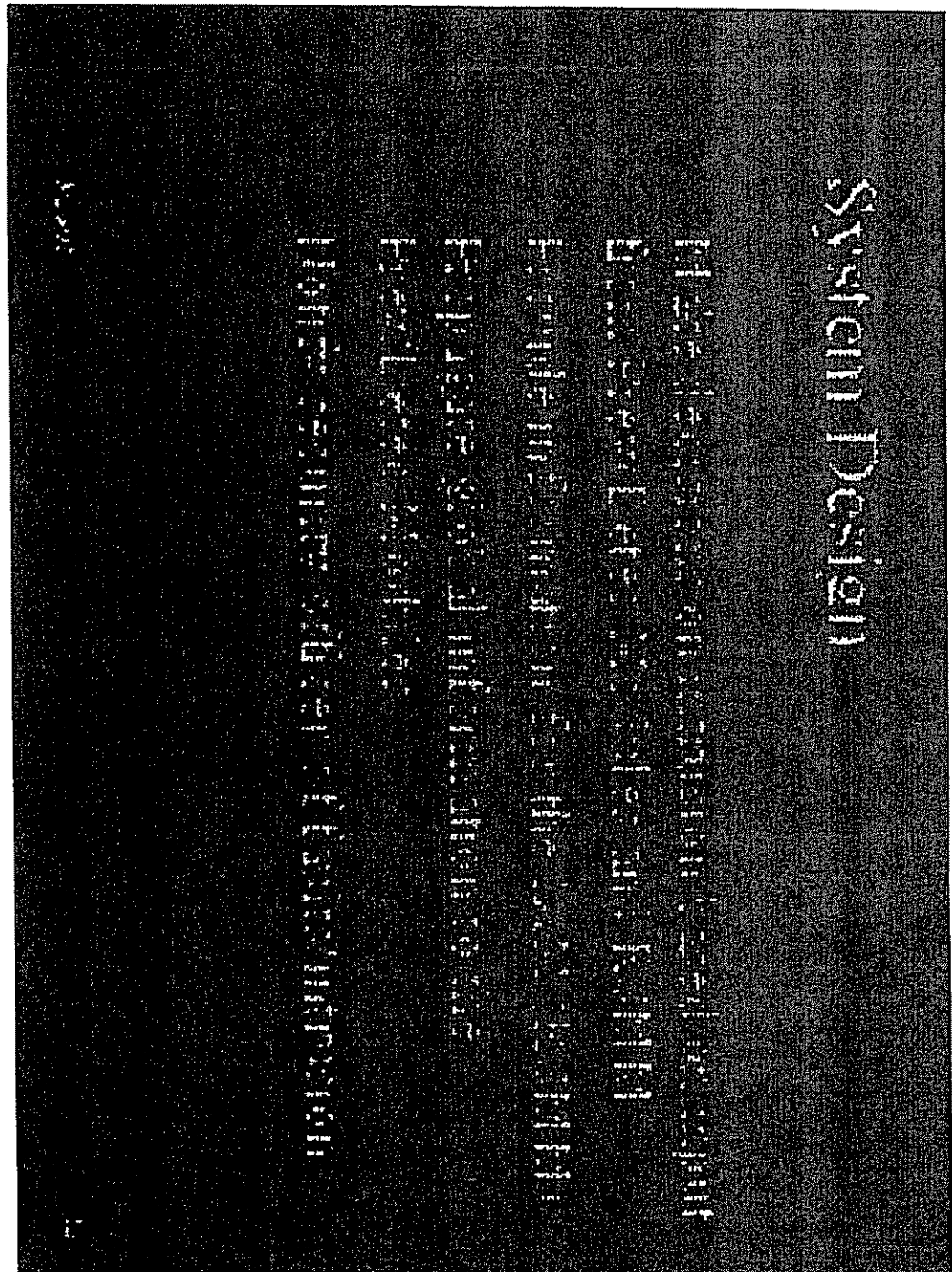
4. Sequence Diagram

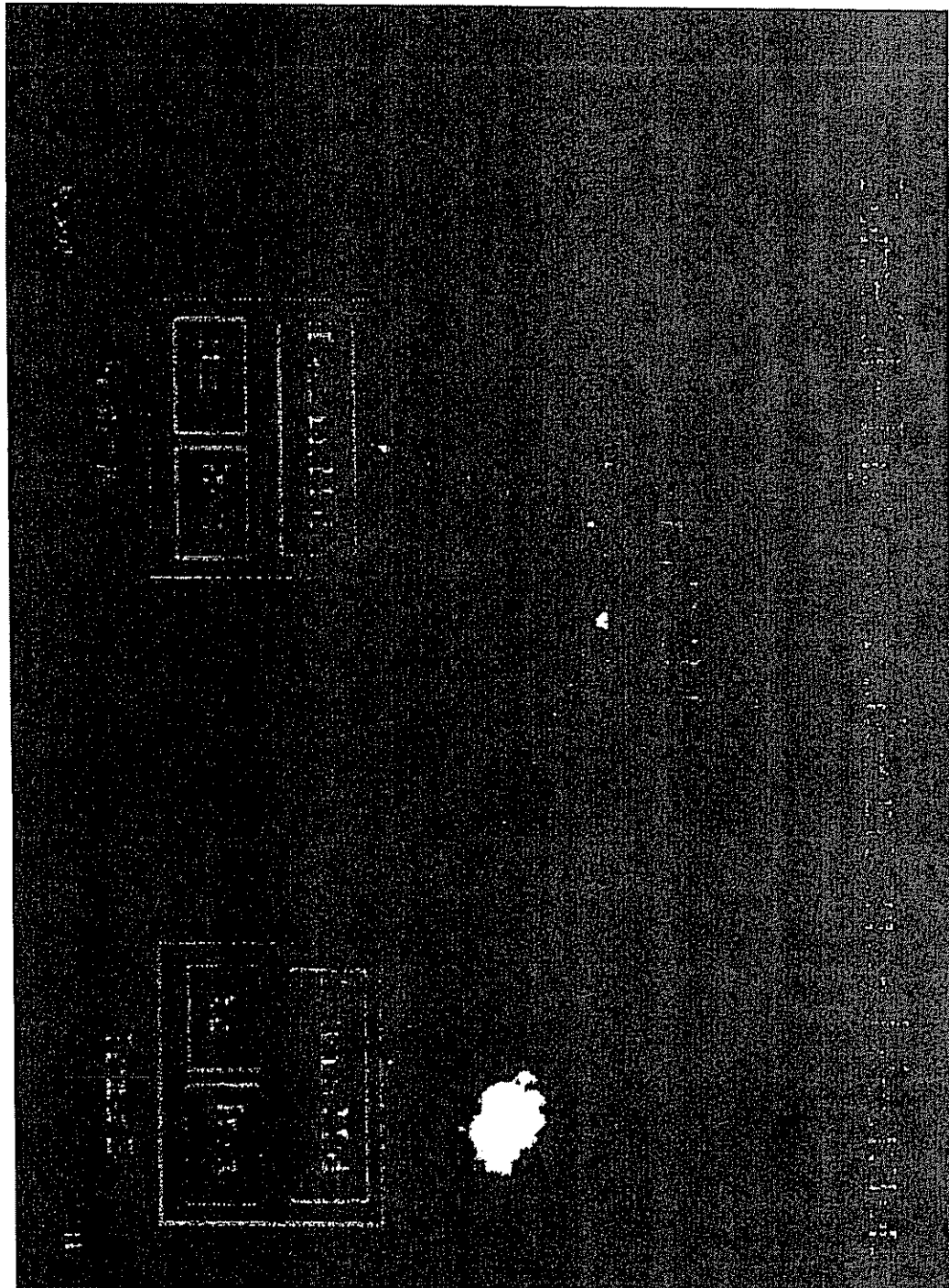
5. Use Case Diagram

6. Deployment Diagram

7. Summary

8. Appendix





System Design

1. Overview of the System Design

2. Functional Requirements

3. Non-Functional Requirements

4. System Architecture

5. Data Model

6. Security Considerations

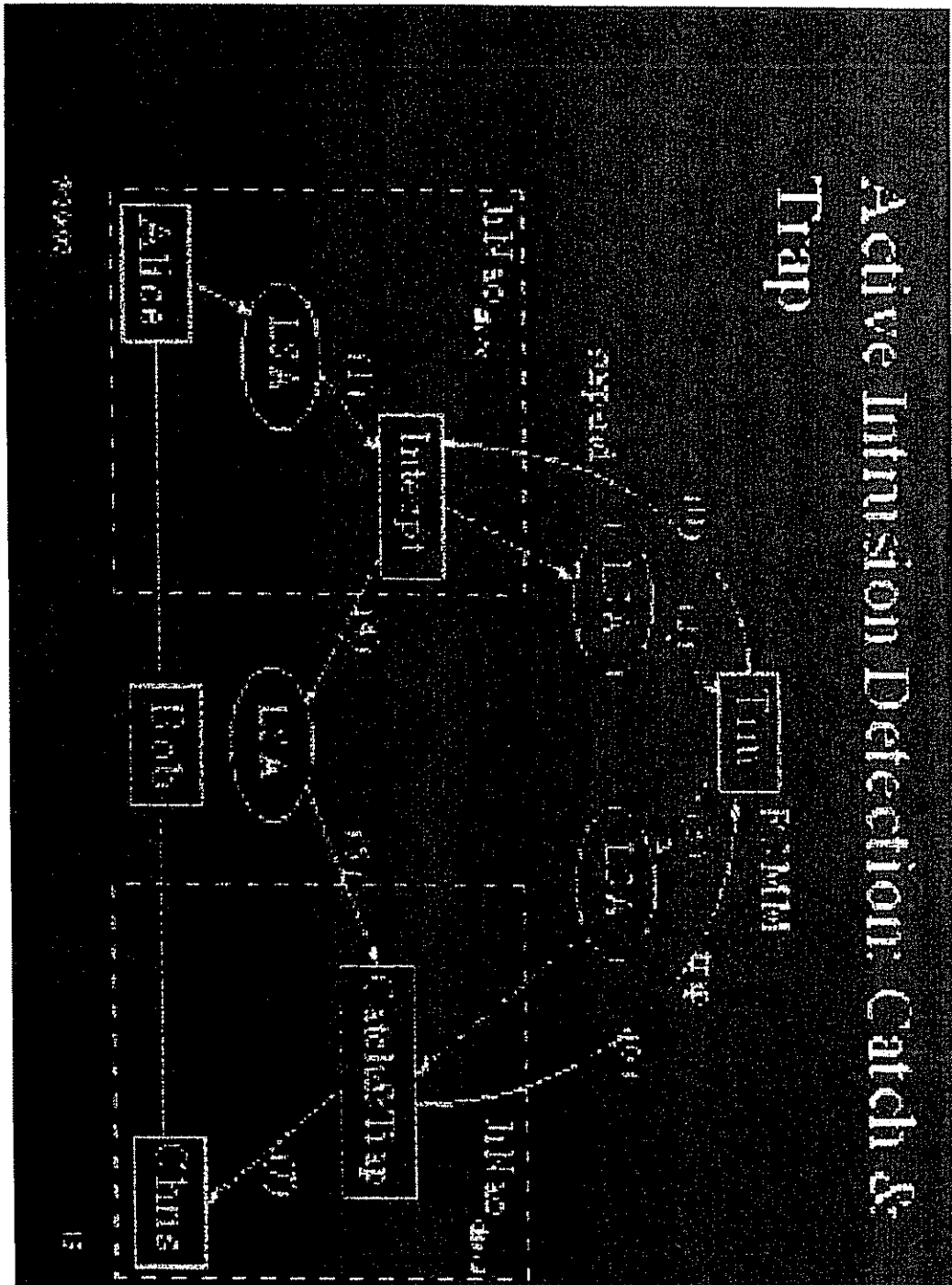
7. Implementation Details

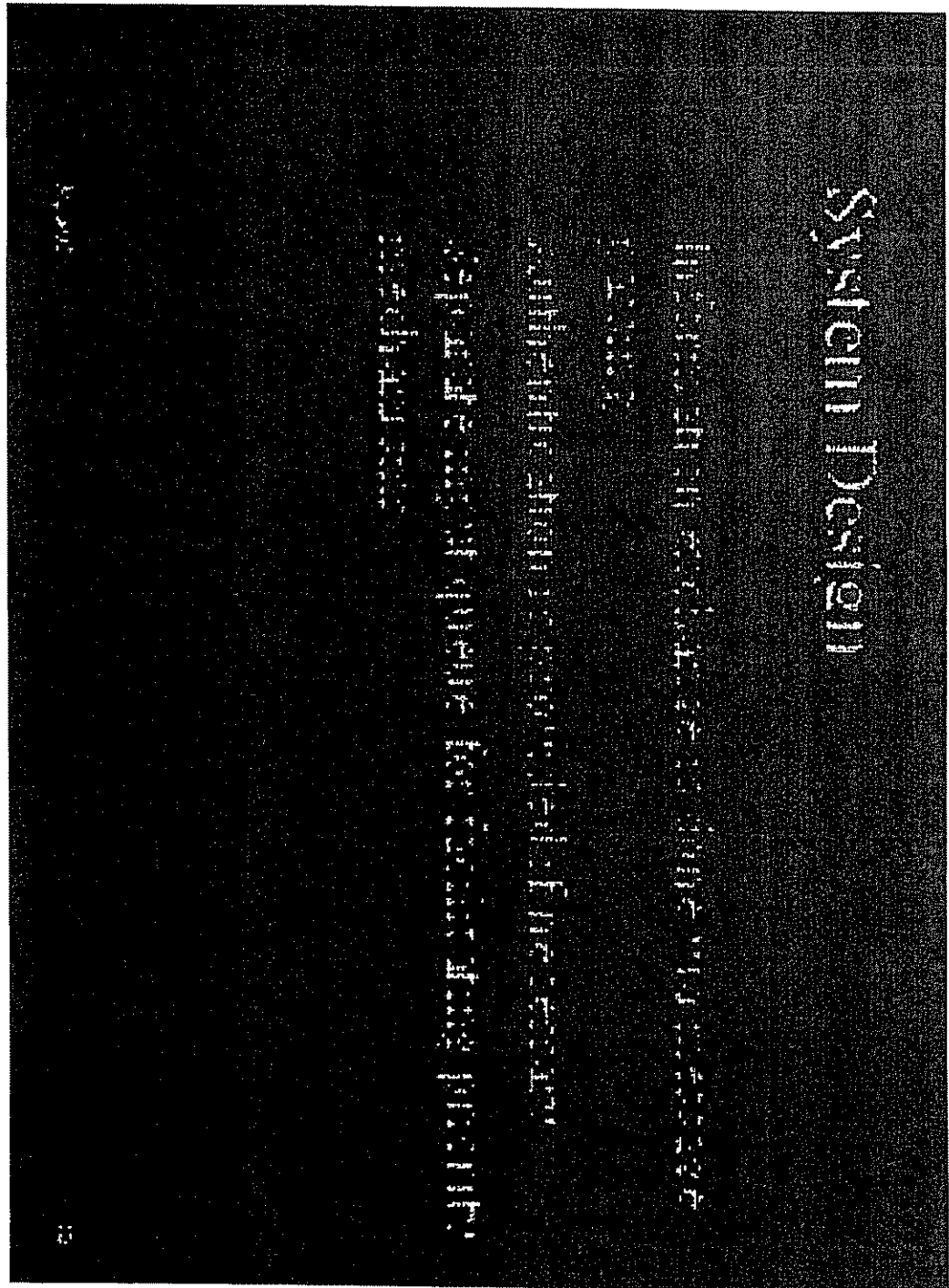
8. Testing Strategy

9. Conclusion

10

Active Intrusion Detection: Catch & Trap





Testbed Configuration

Two running testbeds (autonomous systems, ASes) MICHIE & MESSI

Each has three to four areas

Allow independent code development

Will be linked together to experiment

ASes attached to the external LSes are

flashed throughout the entire AS

(Ref. configuration in file "testbed.pdf")

Next

10

Routing Statistical Profiles

Hello packets stable like step function.
Database Lookup and L3 Request
packets are erratic for forming
any pattern.

L3 Update and L3 Ack packets about
every 30 min. L3 Refreshing 30 min.
MHL Statistics 1 sec.

(Look for four other ports, not Hex, two
were normal, two were under attack)

xxx

Routine Attacks

These are the most common attacks on a system.

They are the most common attacks on a system.

These are the most common attacks on a system.

They are the most common attacks on a system.

These are the most common attacks on a system.

They are the most common attacks on a system.

These are the most common attacks on a system.

